NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)	[Emergency Services](#)
[Regional](#)	[Energy](#)
[National](#)	[Food and Agriculture](#)
[International](#)	[Government Sector (including Schools and Universities)](#)
[Banking and Finance Industry](#)	[Information Technology and Telecommunications](#)
[Chemical and Hazardous Materials Sector](#)	[Public Health](#)
[Commercial Facilities](#)	[Transportation](#)
[Communications Sector](#)	[Water and Dams](#)
[Critical Manufacturing](#)	[North Dakota Homeland Security Contacts](#)
[Defense Industrial Base Sector](#)	

NORTH DAKOTA

(North Dakota) North Dakota launches oil rules hoping to curb U.S. rail disasters. The governor of North Dakota announced April 1 that the State will require the more-than 1.2 million barrels of crude extracted each day from the State's Bakken shale formation be removed of volatile gases linked to recent crude-by-rail incidents. The crude oil conditioning order requires every barrel of crude to be run through machines that filter for ethane, propane, and other national gas liquids prior to transportation. http://www.msn.com/en-us/news/us/north-dakota-launches-oil-rules-hoping-to-curb-us-rail-disasters/ar-AAaiel1

(North Dakota) Conditions prompt North Dakota governor to declare emergency. Gov. Jack Dalrymple has declared a fire emergency as wildfires continue to flare up around North Dakota. Dry conditions, unseasonably high temperatures and strong winds have led to several grass fires this week. http://newsok.com/conditions-prompt-north-dakota-governor-to-declare-emergency/article/feed/820711

(North Dakota, Minnesota) Dozens of wildfires keep crews busy in northern Minnesota, into North Dakota. Tinder-dry conditions and winds gusting in excess of 50 mph fueled dozens of wildfires across northern Minnesota, although things quieted down on the fire front in North Dakota a bit on Thursday. http://www.grandforksherald.com/news/region/3714070-dozens-wildfires-keep-crews-busy-northern-minnesota-north-dakota

REGIONAL

(Minnesota) Deadly bird flu shows up in South Dakota, 4th Minnesota farm. Federal officials confirmed April 2 the presence of the H5N2 strain of avian flu in a flock of 21,000 at a commercial turkey farm in Nobles County, Minnesota, and in a flock of 53,000 turkeys in Beadle County, South Dakota. The cases bring the total number of outbreaks in the Midwest to 9 and the total number of turkey deaths to 314,000 since early March. http://abcnews.go.com/US/wireStory/4th-minnesota-turkey-farm-infected-deadly-bird-flu-30065188

(Minnesota) Xcel nuclear power unit back online after false fire alarm. Xcel Energy officials reported that the Unit 2 reactor at the Prairie Island Nuclear Generating Plant in Red Wing was back to full power March 28 after workers repaired a ruptured disk in a pressure tank that triggered the plant's fire alarm, affected the cooling and ventilation systems, and prompted the reactor to shut down March 5. http://www.startribune.com/local/298018451.html

(South Dakota) Harding County fire scorches thousands of acres. Crews worked to contain the Sheep Draw fire which burned about 6,430 acres in the West Short Pines area of Harding County, South Dakota, March 30. Several structures including natural gas well sites are in the line of fire and structure crews remained on site to monitor the area. http://www.kotatv.com/news/south-dakota-news/Harding-County-fire-scorches-thousands-of-acres/32089166

NATIONAL

(Maryland) One shot dead at Fort Meade after trying to ram NSA gate. The FBI is conducting an investigation after a U.S. National Security Agency police officer shot and killed one man and seriously injured another while they were attempting to drive into the main gate of the agency's headquarters at Fort Meade, Maryland, March 30. http://www.cnn.com/2015/03/30/us/fort-meade-nsa-incident/index.html

(National) Obama announces executive order on sanctions against hackers. President Barack Obama announced an executive action Wednesday that allows the Treasury Department to impose financially punitive sanctions against cyber hackers who impose a significant threat to national security. http://www.cnn.com/2015/04/01/politics/obama-cyber-hackers-executive-order/

INTERNATIONAL

(Kenya) 147 dead, Islamist gunmen killed after attack at Kenya college. The massacre that killed 147 people and wounded scores of others at a Kenyan university lasted for hours Thursday before the terror was over. The death toll is the highest in a terror attack on Kenyan soil since the U.S. Embassy was bombed in 1998. http://www.cnn.com/2015/04/02/africa/kenya-university-attack/

(International) Google decides to stop trusting CNNIC certificates. Google security engineers announced that the company would no longer allow its Chrome Web browser to recognize digital certificates issued by the China Internet Network Information Center (CNNIC), following an incident during the week of March 23 in which an intermediate certificate authority (CA) operating under CNNIC issued a number of unauthorized digital certificates for Google domains. http://www.net-security.org/secworld.php?id=18164

(International) Lebanese cyberespionage campaign hits defense, telecom, media firms worldwide. Security researchers at Check Point Software Technologies discovered that a cyberespionage group has hacked into hundreds of defense contractor, telecommunications operator, media group, and educational organization networks from at least 10 countries in ongoing attacks that began in late 2012. The attackers detect vulnerabilities and use Web shells to compromise affected servers, including a sophisticated custom-made trojan on servers running Microsoft's IIS software called Explosive that can infect servers and systems on networks and can spread via USB mass storage devices. http://www.networkworld.com/article/2904293/lebanese-cyberespionage-campaign-hits-defense-telecom-media-firms-worldwide.html#tk.rss_all

(International) Trojan Laziok used for reconnaissance in the energy sector. Security researchers from Symantec identified new malware designed for stealing information, dubbed Laziok that was observed targeting users in the petroleum, gas, and helium industries worldwide, and is delivered via a malicious Microsoft Excel file that exploits a buffer overflow/security glitch that allows remote code execution, and downloads custom variants of Cyberat and Zbot malware from servers in the U.S., United Kingdom, and Bulgaria. http://news.softpedia.com/news/Trojan-Laziok-Used-for-Reconnaissance-in-the-Energy-Sector-477175.shtml

(International) Former feds charged with stealing Silk Road bitcoin. A former U.S. Secret Service agent surrendered to authorities March 30 and a U.S. Drug Enforcement Administration agent was arrested March 27 in connection to allegedly stealing over $1.5 million in bitcoins while investigating the Silk Road, a shutdown underground site that traded in illegal drugs, counterfeit IDs, and computer hacking software. The pair, based in Maryland, stole proceeds from the

site and hid the funds in offshore accounts, often utilizing their positions in the government to obtain the bitcoins.
http://www.usatoday.com/story/news/2015/03/30/federal-agents-charged-with-stealing-bitcoin-from-silk-road-case/70672058/

Banking and Finance Industry

(International) Four charged in international Uganda-based cyber counterfeiting scheme. Four suspects were indicted April 2 on charges relating to their roles in a Uganda-based international conspiracy in which they allegedly manufactured, advertised, bought, and sold over $1.4 million in counterfeit U.S. Federal Reserve Notes worldwide via "dark Web" criminal online forums that they created from 2013 – 2014. http://www.justice.gov/opa/pr/four-charged-international-uganda-based-cyber-counterfeiting-scheme

(International) IBM uncovers new, sophisticated bank transfer cyber scam. Security researchers at IBM discovered a sophisticated fraud scheme dubbed "The Dyre Wolf" in which cybercriminals infect users' systems with the Dyrmalware to trick individuals into initiating large wire transfers with criminals posing bank employees over the phone, before moving the funds from bank to bank and usidenial-of-service (DoS) attacks to avoid detection. The scheme has caused losses of over $1 million from multiple large- and medium-sized companies in the U.S. http://www.reuters.com/article/2015/04/02/us-cyberattack-ibm-idUSKBN0MT28Z20150402

(New York) Customs: $730K in fake checks, money orders smuggled into JFK. U.S. Customs and Border Protection officers at New York's John F. Kennedy International Airport seized 516 counterfeit bank and money orders totaling $732,585 in a shipment from the Ivory Coast over the weekend of March 28. The officers deemed the documents fake after noticing that they lacked the necessary security features found in legitimate monetary instruments.
http://patch.com/new-york/fivetowns/customs-730k-fake-checks-money-orders-smuggled-jfk

Chemical and Hazardous Materials Sector

(Florida) EPA takes action to protect the public from an unregistered pesticide / EPA issues order to stop the sale of BioStorm and NanoStrike. The U.S. Environmental Protection Agency (EPA) ordered Saint Augustine-based Nano Defense Solutions, Inc., March 30 to halt sales of its BioStorm and NanoStrike products that the company claims in advertisements are able to kill or repel bacteria or germs, despite having never been tested and registered by the EPA as an approved pesticide.
http://yosemite.epa.gov/opa/admpress.nsf/21b8983ffa5d0e4685257dd4006b85e2/ff5b89a7e378544b85257e18006c9bc3!OpenDocument

Commercial Facilities

(Michigan) Bomb threat leads to evacuation of Bass Pro Shops in Auburn Hills Thursday. A Bass Pro Shops store at the Great Lakes Crossing Outlets in Auburn Hills was evacuated and closed for more than 2 hours April 2 while authorities investigated a phoned bomb threat. The store was cleared to reopen after authorities deemed the incident a false alarm.
http://www.macombdaily.com/general-news/20150403/bomb-threat-leads-to-evacuation-of-bass-pro-shops-in-auburn-hills-thursday

(California) $3.5M in jewels stolen from Temecula business. More than 2,000 pieces of retail jewelry worth about $3.5 million was stolen from the Diamonds by Monet jewelry store in Temecula March 24 after a suspect cut holes into a roof and wall to access the store's office, then used a power saw and jackhammer to break into a safe where the jewelry was held. A reward is being offered for information leading to an arrest. http://abc7.com/news/$35m-in-jewels-stolen-from-temecula-business/602231/

(Minnesota) U.S. Steel cuts more from Minnesota ore. U.S. Steel Corp., announced March 31 that it will idle a portion of its Minnesota Ore Operations Minntac plant in Mt. Iron effective June 1, as part of ongoing company operational adjustments to market conditions. Operations at the Minntac plant will continue at reduced capacity in order to meet customer demand.
http://www.bizjournals.com/pittsburgh/news/2015/03/31/u-s-steel-announces-cuts-more-from-minnesota-ore.html

COMMUNICATIONS SECTOR

Nothing Significant to Report

CRITICAL MANUFACTURING

Nothing Significant to Report

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

(International) Miami drug cop went rogue to aid N.J. trafficking ring, feds say. A former Miami police lieutenant pleaded guilty in New Jersey March 31 to receiving over $160,000 in cash and material goods for aiding a gang by purchasing and transporting firearms, drugs, and drug cash on commercial flights to and from New Jersey, New York, Miami, Ecuador, and the Dominican Republic using his position as a police lieutenant to easily transport the items.
http://www.nj.com/news/index.ssf/2015/04/miami_drug_cop_went_rogue_to_aid_nj_trafficking_ri.html

(Massachusetts; Connecticut) Man gets 2.5 years for fake emergency calls to Connecticut dispatchers. A Massachusetts man pleaded guilty March 30 for showing up to fire scenes in Great Barrington with emergency responder equipment and making several fake radio transmissions which were routed to Litchfield County Dispatch in Connecticut in December 2013 and January 2014. The suspect was arrested in April 2014 and admitted to police in March that his voice was the one on the tapes of the false calls.
http://www.middletownpress.com/general-news/20150331/man-gets-25-years-for-fake-emergency-calls-to-connecticut-dispatchers

Energy

(North Dakota) Oil product spill hits North Dakota wetland. The North Dakota Department of Health reported April 2 that 475 barrels of waste were recovered after an Oasis Petroleum LLC-owned pipeline released about 500 barrels of produced water in Burke County, impacting a nearby wetland. http://www.upi.com/Business_News/Energy-Resources/2015/04/02/Oil-product-spill-hits-North-Dakota-wetland/4731427967631/

Food and Agriculture

(International) Rare bug found at Nogales port of entry. U.S. Customs and Border Protection agriculture specialists intercepted a Claudinerobius slateri, a rare invasive insect, during an inspection of a commercial shipment of celery from Mexico at the Nogales port of entry April 20. The shipment was fumigated and later released into U.S. commerce. http://www.azcentral.com/story/news/12-news/2015/04/01/12-news-nogales-port-of-entry-department-of-homeland-securtity/70780500/

(Minnesota) Farm with Jennie-O ties hit by bird flu outbreak. Officials announced March 27 that a Lac qui Parle County turkey farm with ties to Hormel Foods Corp. subsidiary Jennie-O Turkey Store was struck with the H5N2 avian influenza strain, causing 22,000 birds to die and prompting officials to cull an additional 44,000 turkeys. Jennie-O Officials stated that the affected turkeys were not ready for market and no turkeys with the flu strain entered the food chain. http://www.austindailyherald.com/2015/03/farm-with-jennie-o-ties-hit-by-bird-flu-outbreak/

(California) Health officials warn of raw milk's risks after California illnesses. The California Department of Public Health warned the public of the dangers associated with the consumption of raw milk after six Bay Area residents were diagnosed with campylobacteriosis. A statewide recall of Claravale Farm products from San Benito County was issued March 22 after raw milk and raw cream samples tested positive for campylobacter. http://patch.com/california/lagunaniguel-danapoint/health-officials-warn-raw-milks-risks-after-california-illnesses

Government Sector (including Schools and Universities)

(Georgia) 11 of 12 found guilty in APS cheating trial. Eleven out of 12 educators in Atlanta were found guilty April 1 in connection to conspiring to cheat or concealing cheating in order to boost test scores on the Atlanta Public Schools Criterion-Referenced Competency Test for financial gain. A total of 35 educators were charged in March 2013 following a 2009 investigation that revealed system-wide cheating on the tests. http://www.cbs46.com/story/28622132/aps-educators-wait-for-fate

(Florida) Florida Department of State exposes voter information. The Florida Department of State reported March 31 that the Florida Division of Elections notified 45,173 individuals after 15 compact discs that stored their personal information were delivered to entities ordering them without redacting contact details of certain individuals who are exempt from having their personal information released to the public. Authorities do not believe any of the information will be misused and attributed the error to a malfunction in the automated software used to process record requests. http://news.softpedia.com/news/Florida-Department-of-State-Exposes-Voter-Information-477228.shtml

(Georgia) Four Public Works employees arrested on theft charges. Police arrested and charged four Atlanta Department of Public Works employees March 30 in connection to stealing and selling city-owned metals to recycling centers over the course of several years after an audit found that the city lacked adequate controls for tracking its equipment and that millions of dollars in materials were unaccounted for. Two Department of Watershed Management employees were taken into custody the week of March 23 on similar charges. http://www.ajc.com/news/news/breaking-news/public-works-employees-arrested-on-theft-charges/nkhqw/

Information Technology and Telecommunications

(International) Fourth member of international computer hacking ring pleads guilty to hacking and intellectual property theft conspiracy. An Indiana man pleaded guilty to charges surrounding his role in an international hacking ring that

gained unauthorized access to computer networks of companies including Microsoft Corp., Epic Games Inc., Valve Corporation and ZomStudios, and stole unreleased software, source code, trade secrets, copyrighted worksand financial and other sensitive information. The hacker admitted to transmitting approximately 11,266 log-in credentials from one company, and total losses from thscheme were estimated to range from $100 – $200 million. http://www.fbi.gov/baltimore/press-releases/2015/fourth-member-of-international-computer-hacking-ring-pleads-guilty-to-hacking-and-intellectual-property-theft-conspiracy

(International) **Massive DDoS against GitHub continues.** Systems engineers at GitHub reported that complex, large-scale distributed denial-of-service (DDoS) attacks against the company's servers that started March 26 are ongoing but that all of the Web site's services are available to users. Security researchers from Insight Labs traced the start of the attack to advertising and visitor tracking provided by the Chinese search engine Baidu. http://www.net-security.org/secworld.php?id=18148

(International) **Researchers spot 64-bit version of NewPosThings trojan.** Security researchers at Trend Micro identified a new 64-bit version of the NewPosThings point-of-sale (PoS) malware that infects systems by collecting passwords for virtual network computing (VNC) software and disabling operating system security warnings for certain file extensions, and collects user inputs and payment card information via memory scraping. Experts discovered command and control (C&C) servers used by the trojan associated with internet protocol (IP) addresses at two U.S. airports. http://www.securityweek.com/researchers-spot-64-bit-version-newposthings-trojan

(New Jersey) **Rutgers University trying to restore computer systems after denial-of-service attack.** Rutgers University in New Jersey continued to work March 30 to restore its computer systems following a March 27 distributed denial-of-service (DDoS) attack that caused Internet services to slow down or shut down portions of the university's server. School officials reported that no personal or confidential information was breached in the attack which is still being monitored. http://newyork.cbslocal.com/2015/03/30/rutgers-university-trying-to-restore-computer-systems-after-denial-of-service-attack/

(International) Anonymous proxies used for "Shotgun DDoS" attacks. Security researchers at Incapsula released findings from a one-month study revealing that 20 percent of all Layer 7 application layer distributed denial-of-service (DDoS) attacks from January – February were "Shotgun DDoS" attacks carried out through anonymous proxies to bypass mitigation systems by spreading across multiple internet protocols (IPs) and multiple geo-locations. Approximately 45 percent of the incidents originated from addresses in the Tor anonymity network and 60 percent of them employed Tor's Hammer denial-of-service (DoS) tool, which carries out low-and-slow power-on self-test (POST) attacks. http://news.softpedia.com/news/Anonymous-Proxies-Used-for-Shotgun-DDoS-Attacks-477193.shtml

PUBLIC HEALTH

(National) Maker of tainted medical scopes issues new cleaning guide. Olympus America issued new cleaning guidelines March 26 to U.S. hospitals for its duodenoscopes that have been linked to infections of antibiotic-resistant bacteria in 11 patients at 2 separate Los Angeles hospitals in February. The updated guidelines recommend that hospitals and healthcare facilities use a smaller cleaning brush, to be provided by the company around May 8, and additional flushing steps to remove debris in the scopes. http://trib.com/business/maker-of-tainted-medical-scopes-issues-new-cleaning-guide/article_00cdc1aa-77e2-5389-a849-2836bbcc787f.html

(Denver) Denver VA blames TV station for data breach. The Department of Veterans Affairs (VA) in Denver notified 508 patients April 3 that their names and partial Social Security numbers were contained in a document leaked to a television station that listed veterans' appointments with VA's Denver health care facilities. The VA is investigating the unauthorized disclosure. http://gazette.com/denver-va-blames-tv-station-for-data-breach/article/1549014

(New York) New York doctors accused of using free shoes offer to defraud Medicaid. The Brooklyn District Attorney announced March 31 that 23 New York City doctors and medical workers were charged for allegedly running an insurance fraud scheme that billed Medicaid $7 million in expenses for patients they recruited from homeless shelters and welfare centers between October 2012 and September 2014. The medical professionals promised the recruited patients free

shoes if they produced a Medicaid card and agreed to undergo unnecessary physical therapy and testing. http://www.reuters.com/article/2015/03/31/us-usa-new-york-fraud-idUSKBN0MR2J420150331

Transportation

(California) Woman walking inside fence at San Jose Airport is 5th breach. Police subdued and arrested a woman at the Mineta San Jose International Airport in San Jose March 31 after she allegedly jumped a fence and began walking on the airfield, making it the fifth security breach at the airport in less than a year. http://abcnews.go.com/US/wireStory/woman-walking-inside-fence-san-jose-airport-5th-30050042

(National) JetBlue computer outage causes delays for passengers. JetBlue Airways announced March 30 that a system wide computer outage was resolved, causing delays for thousands of passengers after the airline had to issue handwritten boarding passes. The company stated that customers will likely face delays throughout the day while they worked to get operations back to normal. http://abcnews.go.com/Business/wireStory/jetblue-computer-outage-delays-passengers-30001797

Water and Dams

(California) California imposes first mandatory water restrictions to deal with drought. The governor of California issued an executive order April 1 enforcing a 25 percent reduction on the State's 400 local water supply agencies after claiming that the State's 4-year drought had reached near-crisis proportions. The order will impose varying degrees of cutbacks for homeowners, businesses, farms, and others, while water companies will be required to create restrictions to cut back on water use and monitor for compliance. http://www.nytimes.com/2015/04/02/us/california-imposes-first-ever-water-restrictions-to-deal-with-drought.html

(Montana) Army Corps repairing Orchard Home Levee to protect homes. The U.S. Army Corps of Engineers reported that a $148,000 project to repair a 200-foot damaged segment of the Orchard Homes Levee in Missoula County began March 30 and will be completed by April 3 after the embankment was damaged in

the spring of 2014 due to high flows. The repair work was approved by the U.S. Fish and Wildlife Service in order to prevent potential damage to homes during flood season. http://missoulian.com/news/state-and-regional/army-corps-repairing-orchard-homes-levee-to-protect-homes/article_28d6700e-0b22-575a-bd3f-9243e75f0463.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165